EXPLICIT CHABAUTY OVER NUMBER FIELDS

SAMIR SIKSEK

Abstract. Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ over a number field K of degree d, and denote its Jacobian by J. Denote the Mordell–Weil rank of $J(K)$ by r. We give an explicit and practical Chabauty-style criterion for showing that a given subset $\mathcal{K} \subseteq C(K)$ is in fact equal to $C(K)$. This criterion is likely to be successful if $r \leq d(g-1)$. We also show that the only solutions to the equation $x^2 + y^3 = z^{10}$ in coprime non-zero integers is $(x, y, z) = (\pm 3, -2, \pm 1)$. This is achieved by reducing the problem to the determination of K-rational points on several genus 2 curves where $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt[3]{2})$, and applying the method of this paper.

1. Introduction

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ defined over a number field K, and write J for the Jacobian of C. Suppose that the rank of the Mordell–Weil group $J(K)$ is at most $g-1$. In a pioneering paper, Chabauty [15] proved the finiteness of the set of K-rational points on C. This has since been superceded by Faltings' proof of the Mordell conjecture [28] which gives the finiteness of $C(K)$ without any assumption on the rank of $J(K)$. Chabauty's approach, where applicable, does however have two considerable advantages:

(a) The first is that Chabauty can be refined to give explicit bounds for the cardinality of $C(K)$, as shown by Coleman [18]. Coleman's bounds are realistic, and occasionally even sharp; see for example [36], [30]. Coleman's approach has been adapted to give bounds (assuming some reasonable conditions) for the number of solutions of Thue equations [39], the number of rational points on Fermat curves [40], [41], the number of points on curves of the form $y^2 = x^5 + A$ [57], and the number of rational points on twists of a given curve [56].

(b) The second is that the Chabauty–Coleman strategy can often be adapted to compute $C(K)$, as in [6], [7], [32], [34], [35], [42], [59], and even the K-rational points on the symmetric powers of C [50].

This paper is inspired by a talk [1] given by Joseph Wetherell at MSRI on December 11, 2000. In that talk Wetherell suggested that it should be possible to adapt the Chabauty strategy to compute the set of K-rational points on C provided the rank r of the Mordell–Weil group $J(K)$ satisfies $r \leq d(g-1)$, where $d = [K : \mathbb{Q}]$. Wetherell has never published details of his method which we believe is similar to the one we give here.

Date: October 19, 2010.

2010 *Mathematics Subject Classification.* Primary 11G30, Secondary 14K20, 14C20.

Key words and phrases. Chabauty, Coleman, Curves, Jacobians, Divisors, Differentials, Abelian integrals, Fermat-Catalan, Generalized Fermat.

The author is supported by an EPSRC Leadership Fellowship.

[1] http://msri.org/publications/ln/msri/2000/arithgeo/wetherell/1/banner/01.html

In this paper we give a practical Chabauty-style method for determining $C(K)$ which should succeed if the inequality $r \leq d(g-1)$ holds (but see the discussion at the end of Section 2). We suppose that we have been supplied with a basis $D_1, \ldots, D_r$ for a subgroup of $J(K)$ of full-rank and hence finite index—the elements of this basis are represented as degree 0 divisors on C (modulo linear equivalence). Obtaining a basis for a subgroup of full-rank is often the happy outcome of a successful descent calculation (see for example [14], [29], [44], [46], [47], [51], [53], [54]). Obtaining a basis for the full Mordell–Weil group is often time consuming for genus 2 curves ([31], [33], [52], [55]) and simply not feasible in the present state of knowledge for curves of genus ≥ 3. We also assume the knowledge of at least one rational point $P_0 \in C(K)$. If a search for rational points on C does not reveal any points, then experience suggests that $C(K) = \emptyset$, and the methods of [10], [11] are likely to prove this.

This paper is organized as follows. Section 2 gives a heuristic explanation of why Chabauty's approach should be applicable when the rank r of the Mordell–Weil group satisfies $r \leq g(d-1)$. Section 3 gives a quick summary of basic facts regarding v-adic integration on curves and Jacobians. In Section 4, for $Q \in C(K)$ and a rational prime p, we define a certain neighbourhood of Q in $\prod_{v|p} C(K_v)$ that we call the p-unit ball around Q, and give a Chabauty-style criterion for Q to be the unique K-rational point belonging to this neighbourhood. In Section 5 we explain how to combine our Chabauty criterion with the Mordell–Weil sieve, and deduce a practical criterion for a given set $\mathcal{K} \subseteq C(K)$ to be equal to $C(K)$. In Section 6 we use our method to prove the following theorem.

Theorem 1. *The only solutions to the equation*

$$x^2 + y^3 = z^{10} \tag{1}$$

in coprime integers x, y, z are

$$(\pm 3, -2, \pm 1), \quad (\pm 1, 0, \pm 1), \quad (\pm 1, -1, 0), \quad (0, 1, \pm 1).$$

We note that Dahmen [22, Chapter 3.3.2] has solved the equation $x^2 + z^{10} = y^3$ using Galois representations and level lowering. We have been unable to solve (1) by using Galois representations; the difficulty arises from the additional 'non-trivial' solution $(x, y, z) = (\pm 3, -2, \pm 1)$ which is not present for the equation $x^2 + z^{10} = y^3$. We solve (1) by reducing the problem to determining the K-rational points on several genus 2 curves where K is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt[3]{2})$. For all these genus 2 curves the inequality $r \leq d(g-1)$ is satisfied and we are able to determine the K-rational points using the method of this paper.

Recently, David Brown has given [5] an independent and entirely different proof of Theorem 1. Brown's method is rather intricate, and makes use of elliptic curve Chabauty, mod 5 level lowering and number field enumeration.

We would like to thank Tim Dokchitser for useful discussions and Sander Dahmen for corrections.

2. A Heuristic Explanation of Wetherell's Idea

In this section we explain the heuristic idea behind Chabauty's method and then how the heuristic can be modified for curves over number fields. Let C be a smooth projective curve of genus $g \geq 2$ defined over K. Let J be the Jacobian of C and r the rank of the Mordell–Weil group $J(K)$. Fix a rational point $P_0 \in C(K)$ and let

$\jmath : C \hookrightarrow J$ be the Abel-Jacobi map with base point P_0. We use $\jmath$ to identify C as a subvariety of J.

To explain the usual Chabauty method it is convenient to assume that $K = \mathbb{Q}$. Choose a finite prime p. Inside $J(\mathbb{Q}_p)$ it is clear that

$$C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap J(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})},$$

where $\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ in the p-adic topology. Now $J(\mathbb{Q}_p)$ is a $\mathbb{Q}_p$-Lie group of dimension g, and $\overline{J(\mathbb{Q})}$ is a $\mathbb{Q}_p$-Lie subgroup of dimension at most r. Moreover, $C(\mathbb{Q}_p)$ is a 1-dimensional submanifold of $J(\mathbb{Q}_p)$. If $r + 1 \leq g$ then we expect that the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. It turns out that this intersection is indeed finite if $r \leq g - 1$ and Coleman [18] gives a bound for the cardinality of this intersection under some further (but mild) hypotheses. Moreover, in practice this intersection can be computed to any desired p-adic accuracy.

Now we return to the general setting by letting K be a number field of degree d. Define the Weil restrictions

$$V = \mathrm{Res}_{K/\mathbb{Q}}\, C, \qquad A = \mathrm{Res}_{K/\mathbb{Q}}\, J. \tag{2}$$

Then V is a variety of dimension d and A an abelian variety of dimension gd, both defined over $\mathbb{Q}$. Moreover $\jmath : C \hookrightarrow J$ descends to a morphism $V \hookrightarrow A$ defined over $\mathbb{Q}$ which we use to identify V as a subvariety of A. The Weil restriction defines a bijection between $C(K)$ and $V(\mathbb{Q})$, and

$$\mathrm{rank}\, A(\mathbb{Q}) = \mathrm{rank}\, J(K) = r.$$

Mimicking the previous argument

$$V(\mathbb{Q}) \subseteq V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}.$$

Now $\overline{A(\mathbb{Q})}$ is at most r-dimensional, $V(\mathbb{Q}_p)$ is d-dimensional and the intersection is taking place in the $\mathbb{Q}_p$-Lie group $A(\mathbb{Q}_p)$ of dimension gd. If $r + d \leq gd$ we expect that the intersection is finite. As Wetherell points out, this is not always true. For example, let C be a curve defined over $\mathbb{Q}$ with Mordell–Weil rank $\geq g$. One normally expects that $\overline{J(\mathbb{Q})}$ is g-dimensional. Assume that this is the case. Then the intersection

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

will contain a neighbourhood in $C(\mathbb{Q}_p)$ of the base point P_0 and so will be infinite. Now let V and A be obtained from C and J by first base extending to number field K and then taking Weil restriction back to $\mathbb{Q}$. One has a natural injection

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \hookrightarrow V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$$

proving that the latter intersection is infinite. This is true regardless of whether the inequality $r \leq d(g-1)$ is satisfied. However, for a random curve C defined over a number field K, on the basis for the above heuristic argument, we expect the intersection $V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$ to be finite when the inequality $r \leq d(g-1)$ is satisfied.

A **possibly correct** statement is the following. Let C be a smooth projective curve of genus $g \geq 2$ over a number field K of degree d. Suppose that for every subfield $L \subseteq K$ and for every smooth projective curve D defined over L satisfying $D \times_L K \cong_K C$, the inequality

$$\mathrm{rank}\, J_D(L) \leq [L : \mathbb{Q}](g-1)$$

holds, where J_D denotes the Jacobian of D. Let V and A be given by (2). Then $V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$ is finite.

3. Preliminaries

In this section we summarise various results on p-adic integration that we need. The definitions and proofs can be found in [19] and [20]. For an introduction to the ideas involved in Chabauty's method we warmly recommend Wetherell's thesis [59] and the survey paper of McCallum and Poonen [42], as well as Coleman's paper [18].

3.1. **Integration.** Let p be a (finite) rational prime. Let K_v be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}_v$ be the ring of integers in K_v. Let $\mathcal{W}$ be a smooth, proper connected scheme of finite type over $\mathcal{O}_v$ and write W for the generic fibre. In [19, Section II] Coleman describes how to integrate "differentials of the second kind" on W. We shall however only be concerned with global 1-forms (i.e. differentials of the first kind) and so shall restrict our attention to these. Among the properties of integration (see [19, Section II]) we shall need are the following:

(i) $\displaystyle\int_P^Q \omega = -\int_Q^P \omega,$

(ii) $\displaystyle\int_Q^P \omega + \int_P^R \omega = \int_Q^R \omega,$

(iii) $\displaystyle\int_Q^P \omega + \omega' = \int_Q^P \omega + \int_Q^P \omega',$

(iv) $\displaystyle\int_Q^P \alpha\omega = \alpha \int_Q^P \omega,$

for P, Q, $R \in W(K_v)$, global 1-forms ω, ω' on W, and $\alpha \in K_v$. We shall also need the "change of variables formula" [19, Theorem 2.7]: if $\mathcal{W}_1$, $\mathcal{W}_2$ are smooth, proper connected schemes of finite type over $\mathcal{O}_v$ and $\varrho : W_1 \to W_2$ is a morphism of their generic fibres then

$$\int_Q^P \varrho^* \omega = \int_{\varrho(Q)}^{\varrho(P)} \omega$$

for all global 1-forms ω on W_2 and P, $Q \in W_1(K_v)$.

Now let A be an abelian variety of dimension g over K_v, and write Ω_A for the K_v-space of global 1-forms on A. Consider the pairing

$$\Omega_A \times A(K_v) \to K_v, \qquad (\omega, P) \mapsto \int_0^P \omega. \tag{3}$$

This pairing is bilinear. It is K_v-linear on the left by (iii) and (iv). It is $\mathbb{Z}$-linear on the right; this is a straightforward consequence [19, Theorem 2.8] of the "change of variables formula". The kernel on the left is 0 and on the right is the torsion subgroup of $A(K_v)$; see [4, III.7.6].

3.2. **Notation.** Henceforth we shall be concerned with curves over number fields and their Jacobians. We fix once and for all the following notation:

K	a number field,
C	a smooth projective absolutely irreducible curve defined over K, of genus ≥ 2,
J	the Jacobian of C,
v	a non-archimedean prime of K, of good reduction for C,
K_v	the completion of K at v,
k_v	the residue field of K at v,
$\mathcal{O}_v$	the ring of integers in K_v,
$x \mapsto \tilde{x}$	the natural map $\mathcal{O}_v \to k_v$,
$\mathcal{C}_v$	a minimal regular proper model for C over $\mathcal{O}_v$,
$\tilde{C}_v$	the special fibre of $\mathcal{C}_v$ at v,
Ω_{C/K_v}	the K_v-vector space of global 1-forms on C.

3.3. **Integration on Curves and Jacobians.** For any field extension M/K (not necessarily finite), we shall write $\Omega_{C/M}$ and $\Omega_{J/M}$ for the M-vector spaces of global 1-forms on C/M and J/M respectively. We shall assume the existence of some $P_0 \in C(K)$. Corresponding to P_0 is the Abel–Jacobi map,

$$\jmath : C \hookrightarrow J, \qquad P \mapsto [P - P_0].$$

It is well-known that the pull-back $\jmath^* : \Omega_{J/K} \to \Omega_{C/K}$ is an isomorphism of K-vector spaces [43, Proposition 2.2]. Moreover any two Abel–Jacobi maps differ by a translation on J. As 1-forms on J are translation invariant, the map $\jmath^*$ is independent of the choice of P_0 (see [59, Section 1.4]). Let v be a non-archimedean place for K. The isomorphism $\jmath^*$ extends to an isomorphism $\Omega_{J/K_v} \to \Omega_{C/K_v}$, which we shall also denote by $\jmath^*$. For any global 1-form $\omega \in \Omega_{J/K_v}$ and any two points P, $Q \in C(K_v)$ we have

$$\int_Q^P \jmath^*\omega = \int_{\jmath Q}^{\jmath P} \omega = \int_0^{[P-Q]} \omega,$$

using the properties of integration above. We shall henceforth use $\jmath^*$ to identify Ω_{C/K_v} with Ω_{J/K_v}. With this identification, the pairing (3) with $J = A$ gives the bilinear pairing

$$\Omega_{C/K_v} \times J(K_v) \to K_v, \qquad \left(\omega,\ \left[\sum P_i - Q_i\right]\right) \longmapsto \sum \int_{Q_i}^{P_i} \omega, \tag{4}$$

whose kernel on the right is 0 and on the left is the torsion subgroup of $J(K_v)$. We ease notation a little by defining, for divisor class $D = \sum P_i - Q_i$ of degree 0, the integral

$$\int_D \omega = \sum \int_{Q_i}^{P_i} \omega.$$

Note that this integral depends on the equivalence class of D and not on its decomposition as $D = \sum P_i - Q_i$.

3.4. **Uniformizers.** The usual Chabauty approach when studying rational points in a residue class is to work with a local coordinate (defined shortly) and create power-series equations in terms of the local coordinate whose solutions, roughly speaking, contain the rational points. In our situation we find it more convenient to shift the local coordinate so that it becomes a uniformizer at a rational point in the residue class. Fix a non-archimedean place v of good reduction for C, and a minimal regular proper model $\mathcal{C}_v$ for C over v. Since our objective is explicit

computation, we point out that in our case of good reduction, such a model is simply a system of equations for the non-singular curve that reduces to a non-singular system modulo v. Let $Q \in C(K)$ and let $\tilde{Q}$ be its reduction on the special fibre $\tilde{C}_v$. Choose a rational function $s_Q \in K(C)$ so that the maximal ideal in $\mathcal{O}_{\mathcal{C}_v,\tilde{Q}}$ is (s_Q, π), where π is a uniformizing element for K_v. The function s_Q is called [39, Section 1] a *local coordinate* at Q. Let $t_Q = s_Q - s_Q(Q)$. We shall refer to t_Q, constructed as above, as a *well-behaved uniformizer* at Q. The reason for the name will be clear from Lemma 3.1 below.

Before stating the lemma we define the *v-unit ball around Q* to be

$$\mathcal{B}_v(Q) = \{P \in C(K_v) : \tilde{P} = \tilde{Q}\}. \tag{5}$$

Lemma 3.1. (i) *t_Q is a uniformizer at Q,*
(ii) *$\tilde{t}_Q$ is a uniformizer at $\tilde{Q}$,*
(iii) *Let π be a uniformizing element for K_v. Then t_Q is regular and injective on $\mathcal{B}_v(Q)$. Indeed, t_Q defines a bijection between $\mathcal{B}_v(Q)$ and $\pi\mathcal{O}_v$, given by $P \mapsto t_Q(P)$.*

Proof. Parts (i) and (ii) are clear from the construction. Part (iii) is standard; see for example [39, Section 1] or [59, Sections 1.7, 1.8]. □

3.5. **Estimating Integrals on Curves.**

Lemma 3.2. *Let p be an odd rational prime that does not ramify in K. Let v be a place of K above p. Fix a minimal regular model $\mathcal{C}_v$ for C over $\mathcal{O}_v$. Let $Q \in C(K_v)$ and let $t_Q \in K(C)$ be a well-behaved uniformizer at Q. Let $\omega \in \Omega_{\mathcal{C}_v/\mathcal{O}_v}$, and write*

$$\alpha = \frac{\omega}{dt_Q}\Big|_{t_Q=0}. \tag{6}$$

Then $\alpha \in \mathcal{O}_v$. Moreover, for all $P \in \mathcal{B}_v(Q)$,

$$\int_Q^P \omega = \alpha \cdot t_Q(P) + \beta \cdot t_Q(P)^2 \tag{7}$$

for some $\beta \in \mathcal{O}_v$ (which depends on P).

Proof. We can expand ω (after viewing it as an element in $\Omega_{\hat{\mathcal{O}}_Q}$) as a formal power series

$$\omega = (\alpha_0 + \alpha_1 t_Q + \alpha_2 t_Q^2 + \cdots)dt_Q, \tag{8}$$

where the coefficients α_i are all integers in K_v (see for example [39, Proposition 1.6] or [59, Chapters 1.7, 1.8]); here we have not used the assumption that $t_Q(Q) = 0$, merely that t_Q is a local coordinate at Q. We note that $\alpha = \alpha_0$ and hence integral.

Let $P \in \mathcal{B}_v(Q)$. We can now evaluate the integral (see for example [39, Proposition 1.3])

$$\int_Q^P \omega = \sum_{j=0}^{\infty} \frac{\alpha_j}{j+1} t_Q(P)^{j+1};$$

the infinite series converges since $\mathrm{ord}_v(t_Q(P)) \geq 1$ by part (iii) of Lemma 3.1. Thus (7) holds with

$$\beta = \sum_{j=0}^{\infty} \frac{\alpha_{j+1}}{j+2} t_Q(P)^j.$$

To complete the proof we must show that β is integral. Thus, it is sufficient to show that

$$\mathrm{ord}_v(j+2) \leq j$$

for all $j \geq 0$. But $K_v/\mathbb{Q}_p$ is unramified, and so $\mathrm{ord}_v(j+2) = \mathrm{ord}_p(j+2)$. Hence we need to show that $\mathrm{ord}_p(j+2) \leq j$ for all $j \geq 0$ and all odd primes p. This is now an easy exercise. □

4. Chabauty in a Single Unit Ball

Let C be a smooth projective curve over a number field K. Let J be the Jacobian of C and write r for the rank of the Mordell–Weil group $J(K)$. Let $D_1, \cdots, D_r$ be a basis for a free subgroup of finite index in $J(K)$. Let p a rational prime satisfying the following:

(p1) p is odd
(p2) p is unramified in K,
(p3) every prime v of K above p is a prime of good reduction for the curve C.

For each $v \mid p$ we fix once and for all a minimal regular proper model $\mathcal{C}_v$ for C over $\mathcal{O}_v$. Let $Q \in C(K)$. For $v \mid p$, let $\mathcal{B}_v(Q)$ be as in (5), and define the *p-unit ball around* Q to be

$$\mathcal{B}_p(Q) = \prod_{v|p} \mathcal{B}_v(Q). \tag{9}$$

We will shortly give a criterion for a point $Q \in C(K)$ to be the unique K-rational point in its own p-unit ball.

To state our criterion—Theorem 2 below—we need to define a pair of matrices T and A. The matrix T depends on the basis $D_1, \ldots, D_r$. The matrix A depends on the point $Q \in C(K)$. Let $v_1, \ldots, v_n$ be the places of K above p. For each place v above p we fix once and for all a $\mathbb{Z}_p$-basis $\theta_{v,1}, \ldots, \theta_{v,d_v}$ for $\mathcal{O}_v$, where $d_v = [K_v : \mathbb{Q}_p]$. Of course $d_v = [\mathcal{O}_v : \mathbb{Z}_p] = [k_v : \mathbb{F}_p]$ as p is unramified in K. We also choose an $\mathcal{O}_v$-basis $\omega_{v,1}, \ldots, \omega_{v,g}$ for $\Omega_{\mathcal{C}_v/\mathcal{O}_v}$.

Now fix v above p, and let $\omega \in \Omega_{\mathcal{C}_v/\mathcal{O}_v}$. Let

$$\tau_j = \int_{D_j} \omega, \qquad j = 1, \ldots, r. \tag{10}$$

Write

$$\tau_j = \sum_{i=1}^{d_v} t_{ij}\theta_{v,i}, \qquad t_{ij} \in \mathbb{Q}_p. \tag{11}$$

Let

$$T_{v,\omega} = (t_{ij})_{i=1,\ldots,d_v,\ j=1,\ldots,r}; \tag{12}$$

that is $T_{v,\omega}$ is the $d_v \times r$ matrix with entries t_{ij}. Recall that $\omega_{v,1}, \ldots, \omega_{v,g}$ is a basis for $\Omega_{\mathcal{C}_v/\mathcal{O}_v}$. Let

$$T_v = \begin{pmatrix} T_{v,\omega_{v,1}} \\ T_{v,\omega_{v,2}} \\ \vdots \\ T_{v,\omega_{v,g}} \end{pmatrix}; \tag{13}$$

this is a $gd_v \times r$ matrix with entries in $\mathbb{Q}_p$. We now define the matrix T needed for our criterion below:

$$T = \begin{pmatrix} T_{v_1} \\ T_{v_2} \\ \vdots \\ T_{v_n} \end{pmatrix}. \tag{14}$$

Note that T is $gd \times r$ matrix with entries in $\mathbb{Q}_p$ where $d = [K : \mathbb{Q}] = d_{v_1} + \cdots + d_{v_n}$.

Let $Q \in C(K)$. We now define the second matrix A needed to state our criterion for $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$. For each place v of K above p, we have chosen a minimal proper regular model $\mathcal{C}_v$. Let t_Q be a well-behaved uniformizer at Q as defined in Subsection 3.4. Let $\omega \in \Omega_{\mathcal{C}_v/\mathcal{O}_v}$ and let α be given by (6). By Lemma 3.2, $\alpha \in \mathcal{O}_v$. Recall that we have fixed a basis $\theta_{v,1}, \ldots, \theta_{v,d_v}$ for $\mathcal{O}_v/\mathbb{Z}_p$. Write

$$\alpha \cdot \theta_{v,j} = \sum_{i=1}^{d_v} a_{ij} \theta_{v,i}, \qquad j = 1, \ldots, d_v, \tag{15}$$

with $a_{ij} \in \mathbb{Z}_p$. Let

$$A_{v,\omega} = (a_{ij})_{i,j=1,\ldots,d_v}. \tag{16}$$

Let

$$A_v = \begin{pmatrix} A_{v,\omega_1} \\ A_{v,\omega_2} \\ \vdots \\ A_{v,\omega_g} \end{pmatrix}; \tag{17}$$

this is a $d_v g \times d_v$ matrix with entries in $\mathbb{Z}_p$. Let

$$A = \begin{pmatrix} A_{v_1} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & A_{v_2} & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & A_{v_n} \end{pmatrix}. \tag{18}$$

Then A is a $dg \times d$ matrix with entries in $\mathbb{Z}_p$.

We use A and T to define a matrix $M_p(Q)$ in terms of which we will express our criterion for Q to be the unique rational point in its p-unit ball. Choose a non-negative integer a such that $p^a T$ has entries in $\mathbb{Z}_p$. Let U be a unimodular matrix with entries in $\mathbb{Z}_p$ such that $U(p^a T)$ is in Hermite Normal Form. Let h be the number of zero rows of $U(p^a T)$. Let $M_p(Q)$ be the $h \times d$ matrix (with entries in $\mathbb{Z}_p$) formed by the last h rows of UA.

Theorem 2. *With the above assumptions and notation, denote by $\tilde{M}_p(Q)$ the matrix with entries in $\mathbb{F}_p$ obtained by reducing $M_p(Q)$ modulo p. If $\tilde{M}_p(Q)$ has rank d then $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$.*

Remarks.

(i) Let $\mathbf{u}_1, \ldots, \mathbf{u}_h$ be a $\mathbb{Z}_p$-basis for the kernel of the homomorphism of $\mathbb{Z}_p$-modules $\mathbb{Z}_p^{gd} \to \mathbb{Z}_p^r$ given by $p^a T$. Then $\mathbf{u}_1 A, \ldots, \mathbf{u}_h A$ span the same $\mathbb{Z}_p$-module the rows of $M_p(Q)$, showing that the rank of $\tilde{M}_p(Q)$ is independent of the choice of U.

(ii) Since the matrix T is $gd \times r$, it is evident that $h \geq \max(gd-r, 0)$ and, very likely, $h = \max(gd-r, 0)$. Now the matrix $\tilde{M}_p(Q)$ is $h \times d$ and so a necessary condition for the criterion to hold is that $h \geq d$. Thus it is sensible to apply the theorem when $gd - r \geq d$, or equivalently when $r \leq d(g-1)$.

(iii) In practice, we do not compute the matrix T exactly, merely an approximation to it. Thus we will not be able to provably determine h unless $h = \max(gd-r, 0)$.

Proof of Theorem 2. Suppose that $P \in C(K) \cap \mathcal{B}_p(Q)$. We need to show that $P = Q$.

Let m be the index

$$m := [J(K) : \langle D_1, \cdots, D_r \rangle]. \tag{19}$$

There are integers $n_1', \ldots, n_r'$ such that

$$m(P-Q) = n_1' D_1 + \cdots + n_r' D_r, \tag{20}$$

where the equality takes place in $\mathrm{Pic}^0(C)$.

Let υ be one of the places $\upsilon_1, \ldots, \upsilon_n$ above p. Recall that we have chosen a well-behaved uniformizer t_Q at Q. Write $z = t_Q(P)$. By part (iii) of Lemma 3.1, $\mathrm{ord}_\upsilon(z) \geq 1$. We will show that $z = 0$, and so again by part (iii) of Lemma 3.1, $P = Q$ which is what we want to prove.

We write

$$z = z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon},$$

where $z_{\upsilon,i} \in \mathbb{Z}_p$. As $\tilde{\theta}_{\upsilon,1}, \ldots, \tilde{\theta}_{\upsilon,d_\upsilon}$ is a basis for $k_\upsilon/\mathbb{F}_p$ and $\mathrm{ord}_\upsilon(z) \geq 1$, we see that $\mathrm{ord}_\upsilon(z_{\upsilon,i}) \geq 1$ for $i = 1, \ldots, d_\upsilon$. Let

$$s_\upsilon = \min_{1 \leq i \leq d_\upsilon} \mathrm{ord}_p(z_{\upsilon,i}). \tag{21}$$

We will show that $s_\upsilon = \infty$, which implies that $z_{\upsilon,i} = 0$ for $i = 1, \ldots, d_\upsilon$ and so $z = 0$ as required. For now we note that $s_\upsilon \geq 1$.

Now fix an $\omega \in \Omega_{\mathcal{C}_\upsilon/\mathcal{O}_\upsilon}$ and let $\alpha \in \mathcal{O}_\upsilon$ be as in Lemma 3.2; by that lemma

$$\int_Q^P \omega = \alpha z + \beta z^2,$$

for some $\beta \in \mathcal{O}_\upsilon$. However, by equation (20) and the properties of integration explained in Section 3,

$$m \int_Q^P \omega = n_1' \tau_1 + \cdots + n_r' \tau_r,$$

where the τ_j are given in (10). Let $n_i = n_i'/m \in \mathbb{Q}$. Thus

$$\int_Q^P \omega = n_1 \tau_1 + \cdots + n_r \tau_r.$$

Hence

$$n_1\tau_1 + \cdots + n_r\tau_r = \alpha(z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon}) + \beta(z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon})^2. \tag{22}$$

From (22) and (21) we obtain

$$n_1\tau_1 + \cdots + n_r\tau_r \equiv z_{\upsilon,1}(\alpha\theta_{\upsilon,1}) + \cdots + z_{\upsilon,d_\upsilon}(\alpha\theta_{\upsilon,d_\upsilon}) \pmod{p^{2s_\upsilon}\mathcal{O}_\upsilon}. \tag{23}$$

Write

$$\mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{pmatrix}, \qquad \mathbf{z}_\upsilon = \begin{pmatrix} z_{\upsilon,1} \\ z_{\upsilon,2} \\ \vdots \\ z_{\upsilon,d_\upsilon} \end{pmatrix},$$

and note that the entries of $\mathbf{n}$ are in $\mathbb{Q}$, and the entries of $\mathbf{z}_\upsilon$ are in $p^{s_\upsilon}\mathbb{Z}_p$. Recall that we have expressed $\tau_j = \sum t_{ij}\theta_{\upsilon,i}$ in (11) and $\alpha \cdot \theta_{\upsilon,j} = \sum a_{ij}\theta_{\upsilon,i}$ in (15) where t_{ij} are in $\mathbb{Q}_p$ and the a_{ij} are in $\mathbb{Z}_p$. Substituting in (23) and comparing the coefficients for $\theta_{\upsilon,i}$ we obtain

$$T_{\upsilon,\omega}\mathbf{n} \equiv A_{\upsilon,\omega}\mathbf{z}_\upsilon \pmod{p^{2s_\upsilon}},$$

where $T_{\upsilon,\omega}$ and $A_{\upsilon,\omega}$ are respectively given in (12) and (16).

Let T_υ and A_υ be as given in (13) and (17) respectively. Then

$$T_\upsilon\mathbf{n} \equiv A_\upsilon\mathbf{z}_\upsilon \pmod{p^{2s_\upsilon}}.$$

Now let

$$\mathbf{z} = \begin{pmatrix} \mathbf{z}_{\upsilon_1} \\ \mathbf{z}_{\upsilon_2} \\ \vdots \\ \mathbf{z}_{\upsilon_n} \end{pmatrix}.$$

Then $\mathbf{z}$ is of length $d = [K : \mathbb{Q}]$ with entries in $p\mathbb{Z}_p$. Write

$$s = \min_{\upsilon=\upsilon_1,\ldots,\upsilon_n} s_\upsilon = \min_{i,j} \operatorname{ord}_{\upsilon_j}(z_{i,\upsilon_j}), \tag{24}$$

where the s_υ are defined in (21). Clearly $s \geq 1$. It is sufficient to show that $s = \infty$ since then all of the $z_{i,\upsilon_j} = 0$ implying that $P = Q$.

Let T and A be as given in (14) and (18). Then

$$T\mathbf{n} \equiv A\mathbf{z} \pmod{p^{2s}}, \tag{25}$$

where we note once again that T is $dg \times r$ with entries in $\mathbb{Q}_p$ and A is $dg \times d$ with entries in $\mathbb{Z}_p$.

Let U, $M_p(Q)$, h be as in the paragraph preceding the statement of the theorem. Suppose that $\tilde{M}_p(Q)$ has rank d. Suppose $s < \infty$ and we will derive a contradiction. Recall that the last h rows of UT are zero. From (25) we have that $M_p(Q)\mathbf{z} \equiv 0 \pmod{p^{2s}}$ since, by definition, $M_p(Q)$ is the matrix formed by the last h rows of UA. In particular M_p has coefficients in $\mathbb{Z}_p$ since both U and A have coefficients in $\mathbb{Z}_p$. From the definition of s in (24) we can write $\mathbf{z} = p^s\mathbf{w}$ where the entries of $\mathbf{w}$ are in $\mathbb{Z}_p$ and $\mathbf{w} \not\equiv \mathbf{0} \pmod{p}$. However, $M_p(Q)\mathbf{w} \equiv 0 \pmod{p^s}$, and as $s \geq 1$, we have that $M_p(Q)\mathbf{w} \equiv 0 \pmod{p}$. Since $\mathbf{w} \in \mathbb{Z}_p^d$, if $\tilde{M}_p(Q)$ has rank d then $\mathbf{w} \equiv \mathbf{0} \pmod{p}$, giving the desired contradiction. □

5. Chabauty and the Mordell–Weil Sieve

Theorem 2 gives a criterion for showing that a given K-rational point Q on C is the unique K-rational point in its p-unit ball, for a rational prime p satisfying certain conditions.

Let L_0 be a subgroup of $J(K)$ of finite index containing the free subgroup L generated by $D_1, \ldots, D_r$ of the previous section. We can take $L_0 = L$ but for our purpose it is preferable to include the torsion subgroup of $J(K)$ in L_0. The usual p-saturation method [48], [49], [33] shows how to enlarge L_0 so that its index

in $J(K)$ is not divisible by any given small prime p. One expects, after checking p-saturation for all small primes p up to some bound that L_0 is in fact equal to $J(K)$. However, proving that $J(K) = L_0$ requires an explicit theory of heights on the Jacobian J. This is not yet available for Jacobians of curves of genus ≥ 3. For Jacobians of curves of genus 2 there is an explicit theory of heights [31], [33], [52], [55], though the bounds over any number fields other than the rationals are likely to be impractically large.

As usual we assume the existence of some $P_0 \in C(K)$ and denote the associated Abel–Jacobi map by $\jmath$. It is easiest to search for K-rational points on C by taking small linear combinations of the generators of L_0 and checking if they are in the image of $\jmath$. In this way we determine a set $\mathcal{K} \subseteq C(K)$ of known K-rational points, and the challenge is to show that $\mathcal{K}$ is in fact equal to $C(K)$. In this section we show how to combine our Theorem 2 with an adaptation of the Mordell–Weil sieve to give a practical criterion for $\mathcal{K}$ to be equal to $C(K)$. The usual Mordell–Weil sieve [9], [10], [12], [13] assumes knowledge of the full Mordell–Weil group. Our adaptation takes careful account of the fact that we are working with a subgroup of finite (though unknown) index.

Before we give the details we point that substantial improvements can be made to the version of the Mordell–Weil sieve outlined below. It has certainly been sufficient for the examples we have computed so far (including the ones detailed in the next section). But we expect that for some other examples it will be necessary (though not difficult) to incorporate the improvements to the Mordell–Weil sieve found in the papers of Bruin and Stoll [10], [12].

Before stating our criterion we need to set up some notation. Here it is convenient to use the same symbol to denote several different Abel-Jacobi maps associated to the fixed K-rational point P_0 and its images on special fibres. Let υ be of good reduction for C. Denote by red the natural maps

$$\mathrm{red} : C(K) \to C(k_\upsilon), \qquad \mathrm{red} : J(K) \to J(k_\upsilon).$$

Denote by $\jmath$ the Abel–Jacobi map $C(k_\upsilon) \to J(k_\upsilon)$ associated to $\tilde{P}_0$.

Lemma 5.1. *Let L_0 be a subgroup of $J(K)$ of finite index $n = [J(K) : L_0]$. Let $P_0 \in C(K)$ and let $\jmath$ denote the Abel-Jacobi maps associated to P_0 as above. Let $\upsilon_1, \ldots, \upsilon_s$ be places of K, such that each $\upsilon = \upsilon_i$ satisfies the two conditions:*

- *(υ1) υ is a place of good reduction for C,*
- *(υ2) the index n is coprime to $\#J(k_\upsilon)$.*

To ease notation, write k_i for the residue field k_{υ_i}. Define inductively a sequence of subgroups

$$L_0 \supseteq L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots \supseteq L_s$$

and finite subsets $W_0, W_1, \ldots, W_s \subset L_0$ as follows. Let $W_0 = \{\mathbf{0}\}$. Suppose we have defined L_i and W_i where $i \leq s-1$. Let L_{i+1} be the kernel of the composition

$$L_i \hookrightarrow J(K) \to J(k_{i+1}).$$

To define W_{i+1} choose a complete set $\mathcal{Q}$ of coset representatives for L_i/L_{i+1}, and let

$$W'_{i+1} = \{\mathbf{w} + \mathbf{q} : \mathbf{w} \in W_i \quad \textit{and} \quad \mathbf{q} \in \mathcal{Q}\}.$$

Let

$$W_{i+1} = \{\mathbf{w} \in W'_{i+1} : \mathrm{red}(\mathbf{w}) \in \jmath(C(k_{i+1}))\}.$$

Then for every $i = 0, \ldots, s$, and every $Q \in C(K)$, there is some $\mathbf{w} \in W_i$ such that

$$n(\jmath(Q) - \mathbf{w}) \in L_i. \tag{26}$$

Proof. The proof is by induction on i. Since L_0 has index n in $J(K)$, (26) is true with $\mathbf{w} = 0$. Let $i \leq s-1$. Suppose $Q \in C(K)$, $\mathbf{w}' \in W_i$ and $\mathbf{l}' \in L_i$ satisfy

$$n(\jmath(Q) - \mathbf{w}') = \mathbf{l}'. \tag{27}$$

By definition of L_{i+1}, the quotient group L_i/L_{i+1} is isomorphic to a subgroup of $J(k_{i+1})$. It follows from assumption ($\upsilon 2$) that n is coprime to the order of L_i/L_{i+1}. Recall that $\mathcal{Q}$ was defined as a complete set of coset representatives for L_i/L_{i+1}. Thus $n\mathcal{Q}$ is also a set of coset representatives. Hence we may express $\mathbf{l}' \in L_i$ as

$$\mathbf{l}' = n\mathbf{q} + \mathbf{l}$$

where $\mathbf{q} \in \mathcal{Q}$ and $\mathbf{l} \in L_{i+1}$. Let $\mathbf{w} = \mathbf{w}' + \mathbf{q}$. Then $\mathbf{w} \in W'_{i+1}$. By (27), we see that

$$n(\jmath(Q) - \mathbf{w}) = \mathbf{l}' - n\mathbf{q} = \mathbf{l} \in L_{i+1}.$$

To complete the inductive argument all we need to show is that $\mathbf{w} \in W_{i+1}$, or equivalently that $\mathrm{red}(\mathbf{w}) \in \jmath(C(k_{i+1}))$. However, since L_{i+1} is contained in the kernel of $\mathrm{red} : J(K) \to J(k_{i+1})$, we see that

$$n(\jmath(\tilde{Q}) - \mathrm{red}(\mathbf{w})) = 0 \qquad \text{in } J(k_{i+1}).$$

Using the fact that n is coprime to $\#J(k_{i+1})$ once again gives $\mathrm{red}(\mathbf{w}) = \jmath(\tilde{Q})$ as required. □

Theorem 3. *We continue with the above notation and assumptions. Let $L_0 \supseteq L_1 \supseteq \cdots \supseteq L_s$ and $W_0, \ldots, W_s$ be the sequences constructed in Lemma 5.1. Let $\mathcal{K}$ be a subset of $C(K)$. Let $P_0 \in \mathcal{K}$ and let $\jmath$ denote the maps associated to P_0 as above. Suppose that for every $\mathbf{w} \in W_s$ there is a point $Q \in \mathcal{K}$ and a prime p such that the following conditions hold:*

(a) *p satisfies conditions (p1)–(p3) on page 7,*
(b) *(in the notation of the previous section) the matrix $\tilde{M}_p(Q)$ has rank d,*
(c) *the kernel of the homomorphism*

$$J(K) \longrightarrow \prod_{\upsilon \mid p} J(k_\upsilon) \tag{28}$$

contains both the group L_s and the difference $\jmath(Q) - \mathbf{w}$,
(d) *the index $n = [J(K) : L_0]$ is coprime to the orders of the groups $J(k_\upsilon)$ for $\upsilon \mid p$.*

Then $C(K) = \mathcal{K}$.

Proof. Suppose that $P \in C(K)$. We would like to show that $P \in \mathcal{K}$. By Lemma 5.1, there is some $\mathbf{w} \in W_s$ such that $n(\jmath(P) - \mathbf{w}) \in L_s$. Let $Q \in \mathcal{K}$ and prime p satisfy conditions (a)–(d) of the theorem. By (c), L_s is contained in the kernel of (28) and hence

$$n(\jmath(\tilde{P}) - \mathrm{red}(\mathbf{w})) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. Since p satisfies assumption (d), it follows that

$$\jmath(\tilde{P}) - \mathrm{red}(\mathbf{w}) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. But by assumption (c) again,

$$\jmath(\tilde{Q}) - \mathrm{red}(\mathbf{w}) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. It follows that $\tilde{P} = \tilde{Q}$ in $C(k_\upsilon)$ for all $\upsilon \mid p$. Hence $P \in \mathcal{B}_p(Q)$ where $\mathcal{B}_p(Q)$ is the p-unit ball around Q defined in (9). By assumption (b) and Theorem 2 we see that $P = Q \in \mathcal{K}$ completing the proof. □

6. The Generalized Fermat Equation with Signature $(2, 3, 10)$

Let p, q, $r \in \mathbb{Z}_{\geq 2}$. The equation

$$x^p + y^q = z^r \tag{29}$$

is known as the Generalized Fermat equation (or the Fermat–Catalan equation) with signature (p, q, r). As in Fermat's Last Theorem, one is interested in integer solutions x, y, z. Such a solution is called *non-trivial* if $xyz \neq 0$, and *primitive* if x, y, z are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The parametrization of non-trivial primitive solutions for (p, q, r) with $\chi \geq 1$ has now been completed [26]. The Generalized Fermat Conjecture [23], [24] is concerned with the case $\chi < 1$. It states that the only non-trivial primitive solutions to (29) with $\chi < 1$ are

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

The Generalized Fermat Conjecture has been established for many signatures (p, q, r), including for several infinite families of signatures: Fermat's Last Theorem (p, p, p) by Wiles and Taylor [60], [58]; $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [25]; $(2, 4, p)$ by Ellenberg [27] and Bennett, Ellenberg and Ng [2]; $(2p, 2p, 5)$ by Bennett [1]. Recently, Chen and Siksek [16] have solved the Generalized Fermat equation with signatures $(3, 3, p)$ for a set of prime exponents p having Dirichlet density 28219/44928. For an exhaustive survey see [17, Chapter 14]. An older but still very useful survey is [38].

There is an abundance of solutions for Generalized Fermat equations with signatures $(2, 3, n)$, and so this subfamily is particularly interesting. The condition $\chi > 1$ within this subfamily coincides with the condition $n \geq 7$. The cases $n = 7$, 8, 9 are solved respectively in [45], [7] and [8]. The case $n = 10$ appears to be the first hitherto unresolved case within this subfamily and this of course corresponds to equation (1).

In this section we solve equation (1) in coprime integers x, y, z, thereby proving Theorem 1. We shall use the computer package `MAGMA` [3] for all our calculations. In particular, `MAGMA` includes implementations by Nils Bruin and Michael Stoll of 2-descent on Jacobians of hyperelliptic curves over number fields; the algorithm is detailed in Stoll's paper [53]. `MAGMA` also includes an implementation of Chabauty for genus 2 curves over $\mathbb{Q}$.

6.1. Case I: y is odd.

From (1) we immediately see that

$$x + z^5 = u^3, \quad x - z^5 = v^3,$$

where u, v are coprime and odd. Hence $2z^5 = u^3 - v^3$.

Case I.1: $3 \nmid z$

Then

$$u - v = 2a^5, \qquad u^2 + uv + v^2 = b^5,$$

where a, b are coprime integers with $z = ab$. We now use the identity

$$(u-v)^2 + 3(u+v)^2 = 4(u^2+uv+v^2) \tag{30}$$

to obtain $4a^{10} + 3c^2 = 4b^5$, where $c = u+v$. Dividing by $4a^{10}$, we obtain a rational point $(X,Y) = (b/a^2, 3c/2a^5)$ on the genus 2 curve

$$C: \quad Y^2 = 3(X^5 - 1).$$

Using `MAGMA` we are able to show that the Jacobian of this genus 2 curve C has Mordell-Weil rank 0 and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It is immediate that $C(\mathbb{Q}) = \{\infty, (1,0)\}$.

Working backwards we obtain the solutions $(x,y,z) = (0,1,\pm 1)$ to (1).

Case I.2: $3 \mid z$

Recall $2z^5 = u^3 - v^3$ and u, v are odd and coprime. Thus

$$u - v = 2 \cdot 3^4 a^5, \qquad u^2 + uv + v^2 = 3b^5,$$

where $z = 3ab$. Now we use identity (30) to obtain $4 \cdot 3^8 a^{10} + 3c^2 = 12b^5$, where $c = u+v$. Hence we obtain a rational point $(X,Y) = (b/a^2, c/2a^5)$ on the genus 2 curve

$$C: Y^2 = X^5 - 3^7.$$

Let J be the Jacobian of C. Using `MAGMA` we can show that $J(\mathbb{Q})$ is free of rank 1, with generator

$$\left(\frac{-9+3\sqrt{-3}}{2}, \frac{81+27\sqrt{-3}}{2}\right) + \left(\frac{-9-3\sqrt{-3}}{2}, \frac{81-27\sqrt{-3}}{2}\right) - 2\infty.$$

Using `MAGMA`'s built-in Chabauty command we find that $C(\mathbb{Q}) = \{\infty\}$. Working backwards we obtain $(x,y,z) = (\pm 1, -1, 0)$.

6.2. **Case II: y is even.** We would now like to solve (1) with y even, and x, y coprime. Replacing x by $-x$ if necessary we obtain $x \equiv z^5 \pmod 4$.

$$x + z^5 = 2u^3, \qquad x - z^5 = 4v^3,$$

where $y = -2uv$. Hence

$$u^3 - 2v^3 = z^5 \qquad u, v \text{ are coprime and } u, z \text{ are odd.} \tag{31}$$

If $3 \mid z$ then this equation is impossible modulo 9. Hence $3 \nmid z$.

Let $\theta = \sqrt[3]{2}$. We shall work in the number field $K = \mathbb{Q}(\theta)$. This has ring of integers $\mathcal{O}_K = \mathbb{Z}[\theta]$ with class number 1. The unit group is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with $\epsilon = 1 - \theta$ a fundamental unit.

Observe that

$$(u - v\theta)(u^2 + uv\theta + v^2\theta^2) = z^5,$$

where the two factors on the left-hand side are coprime as u, v are coprime and z is neither divisible by 2 nor 3. Hence

$$u - v\theta = \epsilon^s \alpha^5, \qquad u^2 + uv\theta + v^2\theta^2 = \epsilon^{-s}\beta^5, \tag{32}$$

where $-2 \le s \le 2$ and α, $\beta \in \mathbb{Z}[\theta]$ satisfy $z = \alpha\beta$. We now use the identity

$$(u - v\theta)^2 + 3(u + v\theta)^2 = 4(u^2 + uv\theta + v^2\theta^2),$$

to obtain

$$\epsilon^{2s}\alpha^{10} + 3(u + v\theta)^2 = 4\epsilon^{-s}\beta^5.$$

TABLE 1.

s	basis for subgroup of $J_s(K)$ of finite index	$C_s(K)$
-2	$(\theta^2+\theta+1, \theta^2+2\theta+1) - \infty$	∞, $(\theta^2+\theta+1, \pm(\theta^2+2\theta+1))$
-1	$(-\theta^2-\theta-1, 11\theta^2+13\theta+17) - \infty$, $\sum_{i=1,2} (\Phi_i, (2\theta^2+2\theta+3)\Phi_i + 2\theta^2+3\theta+4) - 2\infty$ [a], $\sum_{i=3,4} (\Phi_i, (4\theta^2+6\theta+10)\Phi_i + 9\theta^2+11\theta+13) - 2\infty$ [b]	∞, $\left(\frac{-\theta^2-2\theta-1}{3}, \frac{\pm(\theta^2-\theta+1)}{3}\right)$, $(-\theta^2-\theta-1, \pm(11\theta^2+13\theta+17))$
0	$(1,3) - \infty$, $\left(\frac{\theta^2+2\theta+1}{3}, \frac{10\theta^2+8\theta+13}{3}\right) - \infty$	∞, $\left(\frac{\theta^2+2\theta+1}{3}, \frac{\pm(10\theta^2+8\theta+13)}{3}\right)$, $(1, \pm 3)$
1	$D_1 = (-\theta^2-\theta-1, -40\theta^2-53\theta-67) - \infty$, $D_2 = (-1, 3\theta+3) - \infty$, $D_3 = \sum_{i=5,6} (\Phi_i, (2\theta-2)\Phi_i - \theta + 1) - 2\infty$ [c]	∞, $(-\theta^2-\theta-1, \pm(40\theta^2+53\theta+67))$, $(-1, \pm(3\theta+3))$
2	$\emptyset$	∞

[a] Φ_1, Φ_2 are the roots of $2\Phi^2 + (\theta^2+\theta+2)\Phi + (\theta^2+\theta+2) = 0$.
[b] Φ_3, Φ_4 are the roots of $3\Phi^2 + (4\theta^2+5\theta+4)\Phi + (4\theta^2+5\theta+7) = 0$.
[c] Φ_5, Φ_6 are the roots of $3\Phi^2 + (\theta^2-\theta-2)\Phi + (-2\theta^2+2\theta+1) = 0$.

Let C_s be the genus 2 curve defined over K given by

$$C_s : \quad Y^2 = 3(4\epsilon^{-s}X^5 - \epsilon^{2s}).$$

We see that

$$(X, Y) = \left(\frac{\beta}{\alpha^2}, \frac{3(u+v\theta)}{\alpha^5}\right), \tag{33}$$

is a K-rational point on C_s. To complete our proof of Theorem 1 we need to determine $C_s(K)$ for $-2 \le s \le 2$. Let J_s be the Jacobian of C_s. Using reduction at various places of K we easily showed that the torsion subgroup of $J_s(K)$ is trivial in all cases. The 2-Selmer ranks of $J_s(K)$ are respectively 1, 3, 2, 3, 0 for $s = -2, -1, 0, 2, 1$. We searched for K-rational points on each J_s by first searching for points on the associated Kummer surface. We are fortunate to have found enough independent points in $J_s(K)$ in each case to show that the Mordell–Weil rank is equal to the 2-Selmer rank. In other words we have determined a basis for a subgroup of $J_s(K)$ of finite index, and this is given in Table 1.

Note that in each case the rank $r \le 3 = d(g-1)$ where $d = [K : \mathbb{Q}] = 3$ and $g = 2$ is the genus.

We implemented our method in `MAGMA`. Our program succeeded in determining $C_s(K)$ for all $-2 \le s \le 2$, and the results are given in Table 1. The entire computation took approximately 2.5 hours on a 2.8 GHz Dual-Core AMD Opteron; this includes the time taken for computing Selmer groups and searching for points on the Kummer surfaces. It is appropriate to give more details and we do this for

the case $s = 1$. Let $C = C_1$ and write J for its Jacobian. Let

$$\mathcal{K} = \{\infty,\ P_0,\ P_0',\ P_1,\ P_1'\},$$

where

$$P_0 = (-\theta^2 - \theta - 1, 40\theta^2 + 53\theta + 67), \qquad P_1 = (-1, 3\theta + 3),$$

and P_0', P_1' are respectively the images of P_0, P_1 under the hyperelliptic involution. Let D_1, D_2, D_3 be the basis given in Table 1 for a subgroup of $J(K)$ of finite index. Let $L_0 = \langle D_1, D_2, D_3 \rangle$. Our program verified that the index of L_0 in $J(K)$ is not divisible by any prime < 75. Our program used the point

$$P_0 = (-\theta^2 - \theta - 1, 40\theta^2 + 53\theta + 67)$$

as the base point for the Abel-Jacobi map $\jmath$. The image of $\mathcal{K}$ under $\jmath$ is

$$\jmath(\mathcal{K}) = \{D_1, \quad 0, \quad 2D_1, \quad D_1 + D_2, \quad D_1 - D_2\},$$

where we have listed the elements of $\jmath(\mathcal{K})$ so that they correspond to the above list of points of $\mathcal{K}$. Next our program applied the Mordell–Weil sieve as in Lemma 5.1. The program chose 22 places υ which are places of good reduction for C and such that $\#J(k_\upsilon)$ is divisible only by primes < 75. In the notation of Lemma 5.1,

$$L_{22} = \langle 1386000D_1 + 16632000D_2 + 18018000D_3, \quad 24948000D_2, \quad 24948000D_3 \rangle,$$

and

$$\begin{aligned} W_{22} = \{0,\ D_1 - D_2,\ D_1,\ D_1 + D_2,\ 2D_1,\ D_1 + 12474000D_2 + 87318000D_3, \\ 277201D_1 + 5821200D_2 + 51004800D_3, \quad 277201D_1 - 6652800D_2 - 36313200D_3, \\ -277199D_1 + 6652800D_2 + 36313200D_3, \quad -277199D_1 - 5821200D_2 - 51004800D_3\}. \end{aligned}$$

Next we would like to apply Theorem 3 and so we need primes p satisfying conditions (a)–(d) of that theorem. In particular, our program searches for odd primes p, unramified in K, so that every place $\upsilon \mid p$ is a place of good reduction for C, and $\#J(k_\upsilon)$ is divisible only by primes < 75, and so that L_{22} is contained in the kernel of the homomorphism (28). The smallest prime satisfying these conditions is $p = 109$ which splits completely in K and so there are three degree 1 places υ_1, υ_2, υ_3 above 109. It turns out that

$$J(k_\upsilon) \cong (\mathbb{Z}/110)^2,$$

for $\upsilon = \upsilon_1, \upsilon_2, \upsilon_3$. The reader can easily see that

$$L_{22} \subset 110L_0 \subseteq 110J(K)$$

and so clearly L_{22} is in the kernel of (28) with $p = 109$. Moreover, the reader will easily see that every $\mathbf{w} \in W_{22}$ is equivalent modulo $110L_0$ to some element of $\jmath(\mathcal{K})$. Hence conditions (a), (c), (d) of the Theorem 3 are satisfied for each $\mathbf{w} \in W_{22}$ with $p = 109$. To show that $C(K) = \mathcal{K}$ it is enough to show that $\tilde{M}_{109}(Q)$ has rank 3 for all $Q \in \mathcal{K}$.

It is convenient to take

$$\omega_1 = \frac{dx}{y}, \qquad \omega_2 = \frac{xdx}{y},$$

as basis for the 1-forms on C. With this choice we computed the matrices $\tilde{M}_{109}(Q)$ for $Q \in \mathcal{K}$. For example, we obtained

$$\tilde{M}_{109}(\infty) = \begin{pmatrix} 79 & 64 & 0 \\ 31 & 0 & 0 \\ 104 & 0 & 82 \end{pmatrix} \pmod{109};$$

this matrix of course depends on our choice of U used to compute the Hermite Normal Form on page 8, though as observed in the remarks after Theorem 2, its rank is independent of this choice of U. The matrix $\tilde{M}_{109}(\infty)$ clearly has non-zero determinant and so rank 3. It turns out that the four other $\tilde{M}_{109}(Q)$ also have rank 3. This completes the proof that $C(K) = \mathcal{K}$.

We now return to the general case where $-2 \leq s \leq 2$, and would like to recover the coprime integer solutions u, v to equation (31) from the K-rational points on C_s and hence the solutions (x, y, z) to (1) with y even and $x \equiv z^5 \pmod 4$. From (33) and (32) we see that

$$Y = \frac{3(u + v\theta)}{\alpha^5} = 3\epsilon^s \left(\frac{u + v\theta}{u - v\theta} \right).$$

Thus

$$\frac{u}{v} = \theta \cdot \left(\frac{Y + 3\epsilon^s}{Y - 3\epsilon^s} \right).$$

Substituting in here the values of Y and s from the K-rational points on the curves C_s, the only $\mathbb{Q}$**-rational** values for u/v we obtain are respectively -1, 2, 0, 5/4, 1; these respectively come from the points $(\theta^2 + \theta + 1, -\theta^2 - 2\theta - 1)$, $(-\theta^2 - \theta - 1, -11\theta^2 - 13\theta - 17)$, $(1, -3)$, $(-\theta^2 - \theta - 1, 40\theta^2 + 53\theta + 67)$, $(-1, 3\theta + 3)$. This immediately allows us to complete the proof of Theorem 1.

The reader can find the `MAGMA` code for verifying the above computations at: `http://www.warwick.ac.uk/staff/S.Siksek/progs/chabnf/`

Remarks.

(i) Although our approach solves equation (1) completely, we point out that it is possible to eliminate some cases by using Galois representations and level-lowering as Dahmen [22] does for the equation $x^2 + z^{10} = y^3$. Indeed, by mimicking Dahmen's approach and making use of the work of Darmon and Merel [25], and the so called 'method for predicting the exponents of constants' [17, Section 15.7] we were able to reduce to the case $s = 1$, and it is this case that corresponds to our non-trivial solution $(x, y, z) = (\pm 3, -2, \pm 1)$. It seems however that the approach via Galois representations cannot in the current state of knowledge deal with case $s = 1$.

(ii) Note that to solve our original problem (1), we did not need all K-rational points on the curves C_s, merely those $(X, Y) \in C_s(K)$ with

$$\theta \cdot \left(\frac{Y + 3\epsilon^s}{Y - 3\epsilon^s} \right) \in \mathbb{Q}.$$

This suggests that a higher dimensional analogue of elliptic curve Chabauty [6], [7], [34], [35] should be applicable, and this should give an alternative approach to (1). Although it was not needed here we expect that this idea will be useful in other contexts.

References

[1] M. Bennett, *On the equation* $x^{2n}+y^{2n}=z^5$, J. Théor. Nombres Bordeaux **18** (2006), 315–321.

[2] M. A. Bennett, J. S. Ellenberg and N. C. Ng, *The Diophantine equation* $A^4+2^\delta B^2=C^n$, International Journal of Number Theory **6** (2010), 311–338.

[3] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[4] N. Bourbaki, *Lie Groups and Lie Algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer–Verlag, Berlin, 1998. Translated from French; Reprint of the 1989 English translation.

[5] D. Brown, *Primitive solutions to* $x^2+y^3=z^{10}$, `arXiv:0911.2932v2 [math.NT]`.

[6] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, Dissertation, University of Leiden, Leiden, 1999.

[7] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49.

[8] N. Bruin, *The primitive solutions to* $x^3+y^9=z^2$, Journal of Number Theory **111** (2005), no. 1, 179–189.

[9] N. Bruin and N. D. Elkies, *Trinomials* ax^7+bx+c *and* ax^8+bx+c *with Galois groups of order* 168 *and* $8\cdot 168$, pp. 172–188 of C. Fieker and D. R. Kohel (Eds.), **Algorithmic Number Theory**, 5th International Symposium, ANTS-V, Lecture Notes in Computer Science 2369, Springer-Verlag, 2002.

[10] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: an experiment*, Experimental Mathematics **17** (2008), 181–189.

[11] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*, Mathematics of Computations **78** (2009), 2347–2370.

[12] N. Bruin and M. Stoll, *The Mordell–Weil sieve: proving the non-existence of rational points on curves*, to appear in the LMS Journal of Computing Mathematics.

[13] Y. Bugeaud, M. Mignotte, M. Stoll, S. Siksek and Sz. Tengely, *Integral Points on Hyperelliptic Curves*, Algebra & Number Theory **2** (2008), No. 8, 859–885.

[14] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, L.M.S. lecture notes series **230**, Cambridge University Press, 1997.

[15] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024.

[16] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, Journal of Algebra **322** (2009), 638–656.

[17] H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, GTM **240**, Springer-Verlag, 2007.

[18] R. F. Coleman, *Effective Chabauty*, Duke Mathematical Journal **52** (1985), No. 3, 765–770.

[19] R. F. Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Mathematics **121** (1985), 111–168.

[20] P. Colmez, *Intégration sur les variétés p-adiques*, Astérisque **248** (1998), Société Mathématique de France.

[21] G. Cornell and J. H. Silverman (editors), *Arithmetic Geometry*, Springer-Verlag, 1986.

[22] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, University of Utrecht, PhD thesis, 2008.

[23] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14.

[24] H. Darmon and A. Granville, *On the Equation* $z^m=F(x,y)$ *and* $Ax^p+By^q=Cz^r$, Bull. London Math. Society, **27** (1995), no. 6, 513–543.

[25] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[26] J. Edwards, *A complete solution to* $X^2+Y^3+Z^5=0$, J. reine angew. Math. **571** (2004), 213–236.

[27] J. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4+B^2=C^p$, Amer. J. Math. **126** (2004), 763–787.

[28] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[29] E. V. Flynn, *Descent via isogeny in dimension* 2, Acta Arith. **LXVI.1** (1994), 23–43.

[30] E. V. Flynn, *On a theorem of Coleman*, Manuscripta Math. **88** (1995), 447–456.

[31] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc. **347** (1995), no. 8, 3003–3015.
[32] E. V. Flynn, *A flexible method for applying Chabauty's Theorem*, Compositio Math. **105** (1997), 79–94.
[33] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus* 2 *and the infinite descent*, Acta Arith. **79** (1997), no. 4, 333–352.
[34] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533.
[35] E. V. Flynn and J. L. Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205.
[36] D. Grant, *A curve for which Coleman's effective Chabauty bound is sharp*, Proc. Amer. Math. Soc. **122** (1994), no. 1, 317–319.
[37] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Math. **7** (1998), 1–13.
[38] A. Kraus, *On the Equation* $x^p + y^q = z^r$*: A Survey*, Ramanujan Journal **3** (1999), 315–333.
[39] D. Lorenzini and T. J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), 47–77.
[40] W. G. McCallum, *The arithmetic of Fermat curves*, Math. Ann. **294** (1992), no. 3, 503–511.
[41] W. G. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), no. 3, 565–596.
[42] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, preprint, 14 June 2010.
[43] J. S. Milne, *Jacobian Varieties*, pages 167–212 of [21].
[44] B. Poonen and E. F. Schaefer, *Explicit descent on cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.
[45] B. Poonen, E. F. Schaefer and M. Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2 + y^3 = z^7$, Duke Math. J. **137** (2007), 103–158.
[46] E. F. Schaefer, 2*–descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), 219–232.
[47] E. F. Schaefer and J. L. Wetherell, *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian*, J. Number Theory **115** (2005), 158–175.
[48] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (1995), no. 4, 1501–1538.
[49] S. Siksek, *Descents on Curves of Genus* 1, Ph.D. thesis, University of Exeter, 1995.
[50] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra & Number Theory **3** (2009), No. 2, 209–236.
[51] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$ *and their Jacobians*, J. reine angew. Math. **501** (1998), 171–189.
[52] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), 183–201.
[53] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.
[54] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$*, II*, J. Number Theory **93** (2002), 183–206.
[55] M. Stoll, *On the height constant for curves of genus two, II*, Acta Arith. **104** (2002), 165–182.
[56] M. Stoll, *Independence of rational points on twists of a given curve*, Compositio Math. **142** (2006), 1201–1214.
[57] M. Stoll, *On the number of rational squares at fixed distance from a fifth power*, Acta Arith. **125** (2006), 79–88.
[58] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), no. 3, 553–572.
[59] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, Ph.D. dissertation, University of California at Berkeley, 1997.
[60] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443–551.

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: s.siksek@warwick.ac.uk